AN EFFICIENT AND USER PRIVACY-PRESERVING ROUTING PROTOCOL FOR WIRELESS MESH NETWORKS

JAYDIP SEN*

Abstract. Wireless mesh networks (WMNs) have emerged as a key technology for next generation wireless broadband networks showing rapid progress and inspiring numerous compelling applications. A WMN comprises of a set of mesh routers (MRs) and mesh clients (MCs), where MRs are connected to the Internet backbone through the Internet gateways (IGWs). The MCs are wireless devices and communicate among themselves over possibly multi-hop paths with or without the involvement of MRs. User privacy and security have been primary concerns in WMNs due to their peer-to-peer network topology, shared wireless medium, stringent resource constraints, and highly dynamic environment. Moreover, to support real-time applications, WMNs must also be equipped with robust, reliable and efficient routing protocols so as to minimize the end-to-end latency. Design of a secure and efficient routing protocol for WMNs, therefore, is of paramount importance. In this paper, we propose an efficient and reliable routing protocol that also provides user anonymity in WMNs. The protocol is based on an accurate estimation of the available bandwidth in the wireless links and a robust estimation of the end-to-end delay in a routing path, and minimization of control message overhead. The user anonymity, authentication and data privacy is achieved by application of a novel protocol that is based on Rivest's ring signature scheme. Simulations carried out on the proposed protocol demonstrate that it is more efficient than some of the existing routing protocols.

Key words. Wireless mesh network, user anonymity, bandwidth estimation, end-to-end delay, Rivest ring signature scheme, routing

AMS subject classifications.

1. Introduction.

Wireless mesh networking has emerged as a promising concept to meet the challenges in next-generation wireless networks such as providing flexible, adaptive, and reconfigurable architecture while offering cost-effective solutions to service providers. WMNs are multi-hop wireless networks formed by mesh routers (which form a wireless mesh backbone) and mesh clients. The mesh routers provide a rich radio mesh connectivity which significantly reduces the up-front deployment cost of the network. Mesh routers are typically stationary and do not have power constraints. However, the clients are mobile and energy-constrained. Some mesh routers are designated as gateway routers which are connected to the Internet through a wired backbone. A gateway router provides access to conventional clients and interconnects ad hoc, sensor, cellular, and other networks to the Internet. A mesh network can provide multi-hop communication paths between wireless clients, thereby serving as a community network, or can provide multi-hop paths between the client and the gateway router, thereby providing broadband Internet access to the clients.

As WMNs become an increasingly popular replacement technology for last-mile connectivity to the home networking, community and neighborhood networking, it is imperative to design an efficient resource management system for these networks. Routing is one of the most challenging issues in resource management for supporting real-time applications with stringent QoS requirements. However, most of the existing routing protocols for WMNs are extensions of protocols originally designed for *mobile ad hoc networks* (MANETs) and thus they perform sub-optimally.

This paper presents an efficient and secure routing protocol for WMNs that is able to handle stringent QoS requirements of real-time applications while providing user

*Innovation Lab, Tata Consultancy Services Ltd, Bengal Intelligent Park, Salt Lake Electronics Complex, Kolkata - 700091, INDIA. (jaydip.sen@tcs.com). Questions, comments, or corrections to this document may be directed to that email address.

privacy in a secure way. It involves a very low control overhead and hence provides a high network throughput when the number of data sources in the network is large. While issues such as reduction of control overhead of routing and enhancement of network throughput have been addressed for WMNs in [1], the protocol proposed in this paper is more efficient than those schemes as observed in the simulation results.

The key contributions of the paper are as follows: (i) It exploits network topological information to increase the efficiency of route discovery process and uses *multi-point relay* (MPR) nodes and *circular routing* (discussed in Section 4) to enhance the network throughput by reducing the control overhead. (ii) It computes a reliable link quality estimator and utilizes it in route selection. (iii) It provides a framework for reliable and robust estimation of available bandwidth and end-to-end delay in a routing path so that flow admission with guaranteed QoS for applications can be made. It also ensures that the number of retransmission required is minimized. (iv) It provides a simple mechanism to identify selfish nodes who consume network resources but do not cooperate with other nodes in forwarding packets for others. (v) It presents a novel user anonymization scheme that enables secure authentication of the users while protecting their privacy.

The rest of this paper is organized as follows. Section 2 describes related work on routing in WMNs. Section 3 discusses some important challenges in routing in WMNs. Section 4 describes the details of the proposed routing protocol. Simulation results are presented in Section 5. Finally, Section 6 concludes the paper while highlighting some future scope of work.

2. Related Work. Although significant amount of work has been done on routing in MANETs, very little work has been done for WMNs. Most of the routing protocols for MANETs such as AODV and DSR use hop-count as the routing metric. However, this is approach not well-suited for WMNs. The basic idea in minimizing the hop-count is that it reduces delay and maximizes the throughput. But the assumption here is that the links in the path are either perfect or do not work at all, and all links are of equal bandwidth. A routing scheme that uses the hop-count metric does not take link quality into consideration. A minimum hop-count path has, on the average, longer links between the nodes present in the path compared to a higher hop-count path. This reduces the signal strength received by the nodes in that path and thereby increases the loss ratio at each link [2]. Hence, it is always possible that a two-hop path with a good link quality provides higher throughput than a one-hop path with a poor link quality. Moreover, wireless links usually have asymmetric loss rate [3]. Hence, new routing metrics based on link quality are proposed such *expected transmission count* (ETX),*per-hop round-trip time* (RTT), and per-hop packet pair.

Different approaches have been suggested by researchers for designing routing protocols for WMNs. In [4], a QoS routing over OLSR protocol has been proposed that takes into account metrics such as bandwidth and delay where the source node proactively changes a flow's next hop in response to the change in available bandwidth on its path. In [5], the authors have proposed a *link quality source routing* (LQSR) protocol. It is based on DSR and uses ETX as the routing metric. A new routing protocol called *multi-radio link quality source routing* (MR-LQSR) is proposed in [6]. The process of neighbor node discovery and propagation of link metric are same as those in DSR. However, assignment of link weight and computation of the path weight is different. A QoS enabling routing algorithm for mesh-based wireless LAN architecture has been proposed in [7], where the wireless users form an ad hoc peer-to-peer network. The authors also have proposed a protocol for MANET called *ad hoc*

QoS on-demand routing (AQOR) [8]. In [9], the authors have shown that if a *weighted cumulative expected transmission time* [5] is used in a link state routing protocol, it does not satisfy the *isotonicity* property of the routing protocol and leads to formation of routing loops. To avoid routing loops, an algorithm is proposed that uses *metric of interference and channel switching* (MIC) as the routing metric. The *MeshCluster* architecture [10] addresses important issues in WMNs such as auto-configuration of mesh and client nodes, routing and load balancing in the infrastructure. The routing is performed via AODV-ST, a protocol that proactively maintains spanning trees rooted at the gateways. The mobility of the clients is managed by DHCP protocol.

Some routing protocols for WMNs have been developed by extending the existing routing protocols for MANETS with gateway discovery functionality [11][12][13][14][15] [16] [17]. Since these protocols provide unicast routes, individual routes must be maintained between every mobile node and one of the gateways. Therefore, these protocols scale poorly to the number of nodes in the mesh network.

In [18], scalability to the number of mesh nodes is improved with the uses of location information. However, this kind of information is typically not available in scenarios where the mobile nodes in the mesh network are commodity laptops or hand-held devices.

A problem that is common to most of the routing protocols for MANETs and WMNs is that gateway announcements or gateway requests are prone to vanish due to route breaks, and the recovery procedure is often as expensive as establishing a new route. In contrast, [19] proposes an efficient mechanism to fix broken routes locally. Mosko et al. [20] propose to establish multiple non-disjoint paths for better performance, but again the established routes are unicast and this protocol is not scalable to the number of mesh nodes.

IN [21], a single-hop mesh network architecture has been proposed where mobile clients connect directly to the gateways. However, this approach requires a much higher mesh node density for a comparable wireless coverage. In [22], the authors have proposed an anycast routing (i.e. routing form any mobile node to any gateway in the network) protocol that is designed to scale to the network size and to be robust to node mobility.

In contrast to the above approaches, the proposed protocol performs an on-demand route discovery using multiple metrics like bandwidth, delay, and reliability of the links and provides a routing framework that can support high network throughput with a minimum control overhead.

3. Routing Challenges in WMNs. This section first presents the generic architecture of a WMN and then discusses some specific challenges in designing routing algorithms for such networks.

The architecture of a hierarchical WMN consists of three layers as shown in Fig. 3.1. At the top layers are the *Internet gateways* (IGWs) that are connected to the wired Internet. They form the backbone infrastructure for providing Internet connectivity to the elements in the second level. The entities at the second level are called wireless *mesh routers* (MRs) that eliminate the need for wired infrastructure at every MR and forward their traffic in a multi-hop fashion towards the IGW. At the lowest level are the *mesh clients* (MCs) which are the wireless devices of the users. Internet connectivity and peer-to-peer communications inside the mesh are two important applications for a WMN. Therefore design of an efficient and low-overhead routing protocol that avoids unreliable routes, and accurately estimate the end-to-end delay of a flow along the path from the source to the destination is a major

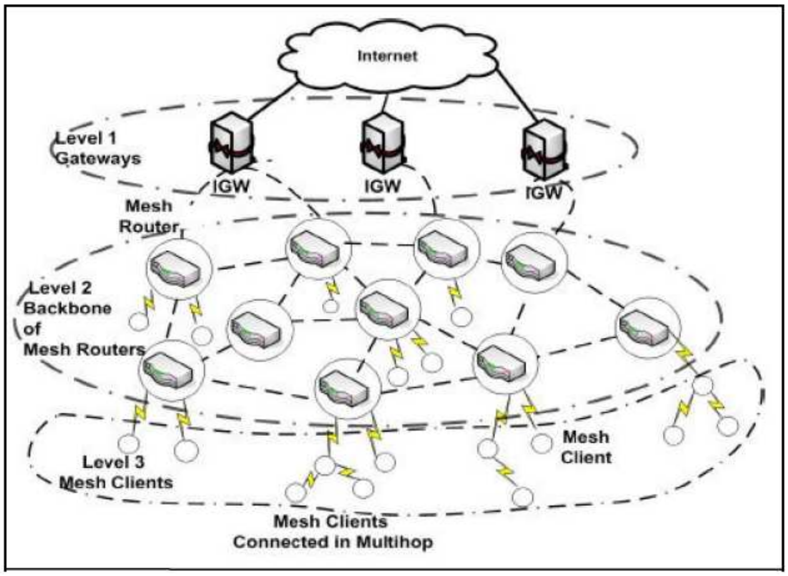

FIG. 3.1. *The three-tier architecture of a wireless mesh network (WMN)*

challenge.

(i) *Measuring link reliability*: It has been observed that in wireless ad hoc networks nodes receiving broadcast messages introduce *communication gray zones* [23]. In such zones, data messages cannot be exchanged although the *hello* messages reach the neighbors. This leads to a disruption in communication among the nodes. Since the routing protocols such as AODV and WMR [7] rely on control packets like RREQ, these protocols are highly unreliable for estimating the quality of wireless links. Due to communication gray zone problem, nodes that are able to send and receive bidirectional RREQ packets sometimes cannot send/receive data packets at high rate. These fragile links trigger link repairs resulting in high control overhead.

(ii) *End-to-end delay estimation*: An important issue in a routing protocol is end-to-end delay estimation. Current protocols estimate end-to-end delay by measuring the time taken to route RREQ and RREP packets along the given path. However, RREQ and RREP are different from normal data packets and hence they are unlikely to experience the same levels of delay and loss as data packets. It has been observed through simulation that a RREP-based estimator overestimates while a hop-count-based estimator underestimates the actual delay experienced by the data packets [24]. The reason for the significant deviation of a RREP-based estimator from the actual end-to-end delay is interference of signals. The RREQ packets are flooded in the network resulting in a heavy burst of traffic. This heavy traffic causes inter-flow interference in the paths. The unicast data packets do not cause such events. Moreover, as a stream of packets traverse along a route, due to the broadcast nature of wireless links, different packets in the same flow interfere with each other resulting in per-packet delays. Since the control packets do not experience per-packet delay, the estimate based on control packet delay deviate widely from the actual delay experienced by the data packets.

(iii) *Reduction of control overhead*: Since the effective bandwidth of wireless channels vary continuously, reduction of control overhead is important in order to maximize

throughput in the network. Reactive protocols like AODV and DSR use flooding of RREQ packets for route discovery. This consumes a high proportion of the network bandwidth and reduces the effective throughput. An important challenge in designing a routing protocol for WMNs is to optimize the communication and computation overhead of the control messages so that the bandwidth of the wireless channels may be used for applications as efficiently as possible. Security and privacy issues bring another dimension of complexity. The goal of the protocol designer would be to design the security framework in such a way that it involves minimum computational and message overhead.

4. The Proposed Routing Protocol. The goal of the proposed routing protocol is to establish a route from a source node to a destination node that allows traffic flow within a guaranteed end-to-end latency and with a guaranteed available bandwidth in the wireless channel using the minimum control overhead. The salient features of the proposed algorithm in this paper are now discussed in the following subsections.

4.1. Estimating Reliability of Routing Paths. Every node estimates the reliability of each of its wireless links to its one-hop neighbor nodes. For computing the reliability of a link, the number of control packets that a node receives in a given time window is used as a base parameter. An *exponentially weighted moving average* (EWMA) method is used to update the link reliability estimate. If the percentage of control packets received by a node over a link in the last interval of measurement of link reliability is N_t, and if N_{t-1} is the historical value of the link reliability before the last measurement interval, $\alpha = 0.5$ is the weighting parameter, then the updated link reliability (R) is computed as in (4.1):

$$R = \alpha.N_t + (1-\alpha).N_{t-1} \tag{4.1}$$

Every node maintains estimates the reliability of each of its links with its neighbors in a *link reliability table*. The reliability for an end-to-end routing path is computed by taking the average of the reliability values of all the links on the path. The use of path with the highest reliability reduces the overhead of route repair. The paths with reliability values less than 0.5 are never selected for routing.

4.2. Use of Network Topological Information in Route Discovery. The proposed protocol makes use of the knowledge of network topology by utilizing selective flooding of control messages in a portion of the network. In this way, broadcasting of control messages is avoided and thus the chances of network congestion and disruption to the flows in the network are reduced. If both the source and the destination are under the control of the same mesh router (refer Fig. 3.1), the flooding of the control messages are confined within the portion of the network served by the mesh router only. However, if the source and the destination are under different mesh routers, the control traffic is limited to the two mesh groups.

To further reduce the overhead of control message and enhance the reliability in routing, the nodes accept broadcast control messages from only those neighbors which have the link reliability value greater than 0.5 (i.e., on average 50% of the control packets sent from those nodes have been received by the node). This ensures that path with less reliability values are not discovered and therefore not considered for routing.

4.3. Estimation of End-to-End Delay in a Routing Path. For accurate estimation of end-to-end delay in a routing path, an approach similar to the one proposed in [24] has been taken. For addressing the issue of differential delays experienced by the control and the data packets, the proposed protocol makes use of some *probe packets* during the route discovery phase. When a source node receives RREP packets from the destination in response to its RREQ, it stores in a table, the records for all the RREP packets together with the path through which the packets have arrived at it. However, instead of randomly selecting a path to send probe packets to the destination as suggested in [24], the packets are sent along the path from which the RREP messages have arrived at the source first. This ensures that the probe packets are sent along the path which is likely to induce less end-to-end delay resulting in a better performance of the protocol as observed from the simulation results presented in Section 5. The probe packets are identical to data packets so far as their size, priority and flow rates are concerned. The objective of sending probe packets is to simulate the data flow and observe the delay characteristics in the routing path. Number of probe packets is kept limited to $2H$ for a path consisting of H hops to make a tradeoff between control overhead and measurement accuracy.

A destination node sets on a timer after it receives the first probe packet from the source node. The timer duration is based on the estimated time for receiving all the probe packets and is computed statistically. The destination computes the average delay experienced by all the probe packets it has received, and sends the computed value to the source node piggybacking it on a RREP message. If the computed value is within the limit of tolerance of the application QoS, the source selects the route and sends data packets. If the delay exceeds the required limit, the source selects the next best path (based on the arrival of RREP packets) from its table and tries once again. Since the routing path is set up based on the probe packets rather than the nave RREP packets, the proposed protocol has higher route establishment The proposed algorithm has higher setup time due to sending of the probe packets and selection of the best path based on the estimated end-to-end delay. However, since the selected paths have high end-to-end reliability, the delay and the control packet overhead are reduced because of minimal subsequent route breaks.

4.4. Use of Multi-Point Relay Nodes. The proposed routing protocol uses the *multi-point relay* (MPR) nodes like the *optimized link state routing* (OLSR) protocol [25] in order to reduce the control overhead in routing. In order to under the concept of MPR let us consider Fig. 3.1.

The control messages sent by an IGW, called GW_INFO messages are never flooded throughout the entire WMN; they are transmitted inside the corresponding subnet (under a particular MR) only. A GW_INFO message is processed by a node if and only if the neighbor which forwarded it has been validated as bi-directional (i.e., the sender is reachable by the receiver via the reverse link). The bi-directionality of a link is determined by appending the list of neighbors in the periodic *hello* messages. In this way, if a node finds itself in the list of neighbors advertised by its own neighbor, the link is considered bi-directional.

This additional list of neighbors in the hello messages is used to compute the MPR of a node. The objective of identifying the MPRs is to minimize control packet overhead. When MPRs are used, it is not necessary to send a message to all the nodes in a network when that message is required to reach all the nodes. If we visualize the WMN as a connected graph, the objective is to find the minimum subset of nodes which covers the whole graph. With a denser network, the benefits of using MPRs

are more prominent. The protocol presented in this paper exploits the advantages of MPRs in order to reduce the control overheads of RREQ messages.

4.5. Estimating Available Network Bandwidth. In addition to computation of path reliability and use of MPRs, it is also necessary that the effective bandwidth in a routing path is reliably estimated. This is extremely important to support real-time applications since these applications require a guarantee for a minimum available bandwidth. In the proposed protocol, the available bandwidth in a wireless link is estimated using its end-to-end delay and loss of packets due to congestion. The packet-loss due to congestion in the link is estimated as follows.In addition to computation of path reliability and use of MPRs, it is also necessary that the effective bandwidth in a routing path is reliably estimated. This is extremely important to support real-time applications since these applications require a guarantee for a minimum available bandwidth. In the proposed protocol, the available bandwidth in a wireless link is estimated using its end-to-end delay and loss of packets due to congestion. The packet-loss due to congestion in the link is estimated as follows.

In a wireless link packet loss may happen due to two reasons: (i) loss due to faulty wireless links and (ii) loss due to network congestion. The *radio link control* (RLC) layer segments an IP packet into several RLC frames before transmission, and reassembles them into an IP packet at the receiver side. An IP packet loss occurs when an RLC frame belonging to an IP packet fails to be delivered. When this happens, the receiver knows the RLC frames reassembly has failed and the IP packet has been lost due to wireless error. Meanwhile, the sender detects *retransmission time out* (RTO) of the frame and discards all the RLC frames belonging to the IP packet. This enables the sender to compute packet drop rate in the wireless links. Moreover, using the sequence numbers of the IP packets received at the receiver, it possible to differentiate the packet loss due to link error and packet loss due to congestion [26]. For example, while receiving two incoming packets with sequence number i and $i+2$, if the receiver finds an IP packet assembly failure in RLC layer, the packet with sequence number $i+1$ is lost due to wireless channel. Once the packet loss ratio due to congestion ($P_{congestion}$) is estimated, the available bandwidth in the wireless link, *estrat*, is given by (4.2) as computed in [26]:

$$estrat = \frac{PacketSize}{(X+Y)} \tag{4.2}$$

X and Y in (4.2) are computed using (4.3) and (4.4) as follows:

$$X = RTT\sqrt{\frac{2P_{congestion}}{3}} \tag{4.3}$$

$$Y = RTO * Min(1, 3\sqrt{\frac{3P_{congestion}}{8}}P_{congestion}(1+32P_{congestion}^2) \tag{4.4}$$

In (4.2), RTT is the average round trip time for a control packet. RTO is the retransmission time out for a packet, and is computed using (4.5).

$$RTO = \overline{RTT} + K.\overline{RTT_{Var}} \tag{4.5}$$

$\overline{RTT}$ and $\overline{RTT_{Var}}$ in are the mean and variance respectively of RTTs and k is set to 4. This bandwidth estimator is employed to dynamically compute the available bandwidth in the wireless links on a routing path so that the guaranteed minimum bandwidth for the flow is always maintained throughout the application life-time.

4.6. Routing through the Fixed Network. In the proposed algorithm, the routing efficiency is further enhanced by occasional routing of packets through the fixed wired network backbone. Since the wired network backbone provides higher available bandwidth with more reliable links, it is advantageously exploited for intra-mesh message communication.

Since the IGWs (refer Fig. 3.1) periodically announce their presence in the network through beacon messages, every mesh client knows the hop count from itself to its selected gateway. In the proposed protocol, the RREQ messages include this hop count information. When the destination receives the RREQ, since it also knows its distance from its gateway, it checks whether it is better (in terms of number of hops) to route the packet through the wireless nodes (mesh) or through the fixed network.

In the proposed protocol, if a destination node finds that the better route is through the fixed network, the RREP message is routed through the wired network using the default route. Therefore, in such situations, the forward route is established between the source and the destination through the wired network, while the reverse route is set up through the WMN. This approach is known as *circular routing* [1]. This approach, improves the performance of bi-directional flows between a source and destination pair (as in a TCP connection) since the nodes in the forward and in the reverse routes are on node-disjoint paths and do not contend for access of the wireless medium.

4.7. Identification of Selfish Nodes. The proposed routing protocol also enforces cooperation among the nodes by identifying the selfish nodes in the network and isolating them. Selfishness is an inherent problem associated with any capacity-constrained multi-hop wireless networks like WMNs. A mesh router can behave selfishly owing to various reasons such as: (i) to obtain more wireless or Internet throughput, or (ii) to avoid path congestion. A selfish mesh router increases the packet delivery latency, and also increases the packet loss rate. A selfish node while utilizing the network resources for routing its own packet, avoids forwarding packets for others to conserve its energy. Identification of selfish nodes is therefore, a vital issue.

Several schemes proposed in the literature to mitigate the selfish behavior of nodes in wireless networks such as credit-based schemes, reputation-based schemes and game theory-based schemes [27]. However, to keep the overhead of computation and communication at the minimum, the proposed protocol employs a simple mechanism to discourage selfish behavior and encourage cooperation among nodes. To punish the selfish nodes, each node forwards packets to its neighbor node for routing only if the link reliability of that node is greater than a threshold (set at 0.5). Since the link reliability of a selfish node is 0, the packets arriving from this node will not be forwarded. Therefore, to keep its link reliability higher than the threshold, each node has to participate and cooperate in routing. The link reliability serves a dual purpose of enhancing reliability and enforcing node cooperation in the network.

4.8. User Anonymity and Privacy. As mentioned in Section 1, the proposed protocol has been augmented with a security module that provides user anonymity and privacy. An *authentication server* (AS) has been used in the network that au-

thenticates the users in the WMN while preserving their privacy. To enable user authentication and anonymity, a novel protocol has been designed extending the improved ring signature authentication scheme in [28].

It is assumed that a symmetric encryption algorithm E exists such that for any key k, the function E_k is a permutation over b-bit strings. We also assume the existence of a family of *keyed combining functions* $C_{k,\nu}(y_1, y_2, ..., y_n)$ [29], and a publicly defined collision-resistant hash function $H(.)$ that maps arbitrary inputs to strings of constant length which are used as keys for $C_{k,\nu}(y_1, y_2, ..., y_n)$. Every keyed combining function $C_{k,\nu}(y_1, y_2, ..., y_n)$ takes as input the key k, an initialization b-bit value ν, and arbitrary values y_1, y_2......,y_n. A user U_i who wants to generate a session key with the authentication server, uses a ring of n logged-on-users and performs the following steps.

Step 1: U_i chooses the following parameters: (i) a large prime p_i such that it is hard to compute the discrete logarithms in $GF(p_i)$, (ii) another large prime q_i such that q_i / (p_i -1), and (iii) a generator g_i in $GF(p_i)$ with order q_i.

Step 2: U_i chooses $x_A \in Z_{q_i}$ as his private key, and computes the public key y_{A_i} = ${g_i}^{x_{A_i}}$ mod p_i.

Step 3: U_i defines a trap-door function:

$$f_i(\alpha, \beta) = \alpha.y_{A_i}^{\alpha mod q_i}.g_i^{\beta} mod p_i$$

Its inverse function $f_i^{-1}(y)$ is defined as: $f_i^{-1} = (\alpha, \beta)$, where α and β are computed as in (4.6), (4.7), and (4.8). In these equations, K is a random integer Z_{q_i}).

$$\alpha = y_{A_i}.g_i^{-K.(g_i^k mod q_i)} mod p_i \tag{4.6}$$

$$\alpha^* = \alpha mod q_i \tag{4.7}$$

$$\beta = K.(g_i^K mod p_i) - x_{A_i}.\alpha^* mod q_i \tag{4.8}$$

U_i makes p_i, q_i, g_i and y_{A_i} public, and keeps x_{A_i} as secret.

The *authentication server* (AS) chooses: (i) a large prime p such that it is hard to compute discrete logarithms in $GF(p)$, (ii) another large prime q such that q / (p -1), (iii) a generator g in $GF(p)$ with order q, (iv) a random integer x_B from Z_q as its private key. The AS computes its public key $y_B = g^{x_B}$mod p and publishes (y_B,p,q,g).

Anonymous authenticated key exchange: The key-exchange is initiated by the user U_i and invloves three rounds to computes a secret session key between U_i and AS. The operations in these three rounds are as follows:

Round 1: When U_i wants to generate a session key on the behalf of n ring users U_1, U_2,......U_n where, $(1 \leq i \leq n)$, U_i does the following:

(i) U_i chooses two random integers x_1, $x_A \in Z_q^*$ and computes the following: $R = g^{X_1} mod\ p$, $Q = y_B^{X_1} mod\ p\ mod\ q$, $X = g^{x_A} mod\ p$ and $l = H(X, Q, V, y_B, I)$.

(ii) U_i chooses a pair of values (α_t, β_t) for every other ring member U_t, $(1 \leq t \leq n, t \neq k)$ in a pseudorandom way, and computes $y_t = f_t(\alpha_t, \beta_t) mod\ p_t$.

(iii) U_i randomly chooses a b-bit initialization value ν, and finds the value of y_i from the equation: $C_{k,\nu}(y_1, y_2, ..., y_n) = \nu$.

(iv) U_i computes $(\alpha_i, \beta_i) = f_i^{-1}(y_i)$ by using the trap-door information of f_i. First, it chooses a random integer $K \in Z_{q_i}$, computes α_i using , and keeps K secret. It then computes α_i^* using (4.7), and finally computes β_i using (4.8) .

(v) $(U_1, U_2, ...U_n, \nu, V, R, (\alpha_1, \beta_1), (\alpha_2, \beta_2)...., (\alpha_n, \beta_n))$ is the ring signature σ on X.

Round 2: AS does the following to recover and verify X from the signature σ.

(i) textitAS computes $Q = R^{X_B} mod\ p\ mod\ q$, recovers X using $X = V.g^Q mod\ p$, and hashes X, Q, V and y_b to recover l, where $l = H(X, Q, V, y_B, I)$.

(ii) textitAS computes $y_t = f_i(\alpha_t, \beta t) mod\ p_i$, for $t = 1, 2, ..., n$.

(iii) AS checks whether $C_{k,v}(y_1, y2, ...y_n) = \nu$. If it is true, AS accepts X as valid; otherwise, AS rejects X. If X is valid, AS chooses a random integer x_b from Z_q^*, and computes the following: If it is true, AS accepts X as valid; otherwise, AS rejects X. If X is valid, AS chooses a random integer xb from , and computes the following: $Y = g^{x_b} mod\ p$, $K_s = X^{x_b} mod\ p$, and $h = H(K_s, X, Y, I)$. AS sends $\{h, Y, I'\}$ to U_i.

Round 3: U_i verifies whether $K_{S'}$ is from the server AS. For this purpose, U_i computes $K_S' = Y^{x_a} mod\ p$, hashes K, X, Y to get $h\prime$ using $h' = H(K_S', X, Y, I)$. If $h'? = h$, U_i accepts K_S as the session key.

Security analysis: The key exchange scheme satisfies the following requirements.

(i)*User anonymity*: For a given signature X, the server can only be convinced that the ring signature is actually produced by at least one of the possible users. If the actual user does not reveal the seed K, the server cannot determine the identity of the user. The strength of the anonymity depends on the security of the pseudorandom number generator. It is not possible to determine the identity of the actual user in a ring of size n with a probability greater than $1/n$. Since the values of k and ν are fixed in a ring signature, there are $(2^b)^{n-1}$ number of $(x_1, x_2, ...x_n)$ that satisfy the equation $C_{k,\nu}(y_1, y_2, ...y_n) = \nu$, and the probability of generation of each $(x_1, x_2, ...x_n)$ is the same. Therefore, the signature can't leak the identity information of the user.

(ii)*Mutual authentication*: In the proposed scheme, not only the server verifies the users, but the users can also verify the server. Because of the hardness of inverting the hash function $f(.)$, it is computationally infeasible for the attacker to determine (α_i, β_i) and hence it is infeasible for him to forge a signature. If the attacker wants to masquerade as the AS, he needs to compute $h = H(K_S, X, Y)$. He requires x_B in order to compute X. However, x_B is the private key of AS to which the attacker has no access. (iii)*Forward secrecy*: The forward secrecy of a scheme refers to its ability to defend leaking of its keys of previous sessions when an attacker is able to catch hold of the key of a particular session. The forward secrecy of a scheme enables it to prevent *replay attacks*. In the proposed scheme, since x_a and x_b are both selected randomly, the session key of each period has not relation to the other periods. Therefore, if the session key generated in the period j is leaked, the attacker can not get any information of the session keys generated before the period j. The proposed protocol is, therefore, resistant to replay attack.

5. Performance Evaluation. The proposed protocol has been implemented in the *Qualnet* network simulator, version 4.5 [30]. The reason for the choice of Qualnet is its ability of handle simulation of complex networks at multiple layers of the protocol stack.It is also suitable for simulation of large-scale dense networks like WMNs. The simulated network consists of 50 and 75 static nodes randomly distributed in the simulation area forming a dense WMN. The WMN topology is shown in Fig. 5.1 where 50 nodes are deployed in the network. out of these 50 nodes, 5 are MRs

and remaining 45 are MCs. Each MR has 9 MCs associated with it. In 75 nodes deployment scenario (which is not shown), each of the 5 MRs has 14 MCs under it.

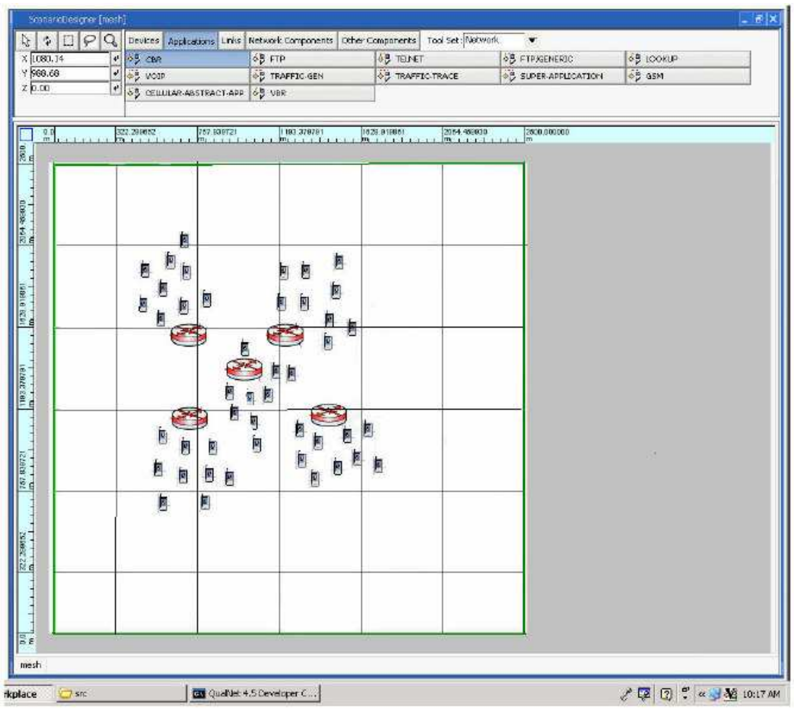

FIG. 5.1. *The simulated WMN topology in Qualnet network simulator*

For connectivity with the backbone Internet, 5 IGWs are placed at locations (100, 100), (100, 1400), (1400, 100) and (1400, 1400) and (700, 700) so as to provide uniform connectivity to backbone Internet with the WMN. The simulation parameters are presented in Table 5.1. The choice of the parameters is made similar to that in [1], and the performances of the two protocols (the proposed protocol and in one presented in [1]) are compared with respect to two important metrics- control packet overhead and network throughput.The overhead due to security and privacy module in the proposed protocol is not considered for the purpose of comparison, since unlike the protocol presented in this paper, the protocol in [1] does not have any security feature. The security and privacy module involves well-known symmetric key encryption, and computations of efficient hash functions and message digests.The computation and communication overhead invloved in these operations are well-known and hence they are not studied in the simulation. The simulation results are presented for the modules which are mainly responsible for efficient operation of the protocol, such as reduction of control message overhead, reduction of end-to-end latency and increasing the network throughput.

5.1. Control Overhead. For studying the control overhead, four algorithms are considered. The DYNMOUM algorithm in [31], the DYNMOUM with MPR, in [1] DYNMOUM with MPR and *circular routing* (CR) [1] and the proposed algorithm compared with respect to their control overhead in routing. The number of data source nodes is varied from 15 to 35 and the control overhead in bytes is studied for

TABLE 5.1
Simulation Parameters

Parameter	Values
Simulated netwoork area	1500m * 1500m
Propagation channel frequency	2.4 GHz
Raw channel bandwidth	2 Mbps
MAC protocol	802.11b
Simulation duration	900 s
Radio range of each node	250 m
Traffic type	CBR UDP
Packet size	512 bytes
Data rate in the network	32 Kbps
IGW hello packet broadcast interval	200 ms
No. of source nodes	15, 25, 35
Node mobility	None
Wireless fading model	None
IP queue scheduler	Strict priority
Propagation model	Two-ray ground
Wired network bandwidth	100 Mbps
Delay in wired links	11.8 ms

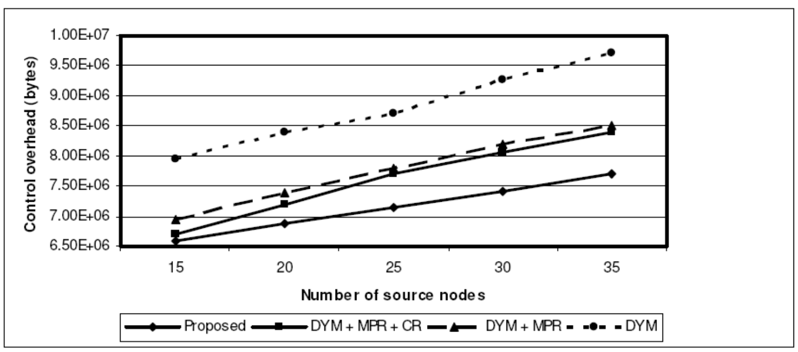

FIG. 5.2. *Control overhead (bytes) vs. number of data source nodes (50 nodes in the networks)*

50 nodes and 75 nodes networks respectively. The results are presented in Fig. 5.2 and Fig. 5.3.

It may be easily observed that the proposed protocol has the least control overhead among all the four protocols. The reason for the less control overhead in the proposed protocol is the less number of route errors and route repairs due the reliable link quality estimation and bandwidth estimation technique used in the protocol, which were absent in the other three protocols. In addition, it exploits the advantages of using MPRs and the circular routing. The MPRs reduce the overhead by controlled flooding and the circular routing reduces the overhead by routing some of the RREPs through the fixed network.

To further demonstrate the efficiency of the proposed protocol, the control packets overhead of the protocol is also compared with that of the protocol presented in [24]. For the purpose of comparison, some changes in the simulation parameters are made. The raw channel bandwidth is set at 11 Mbps. The application traffic is assumed to be CBR UDP. Each flow source is assumed to be sending a maximum of 10,000

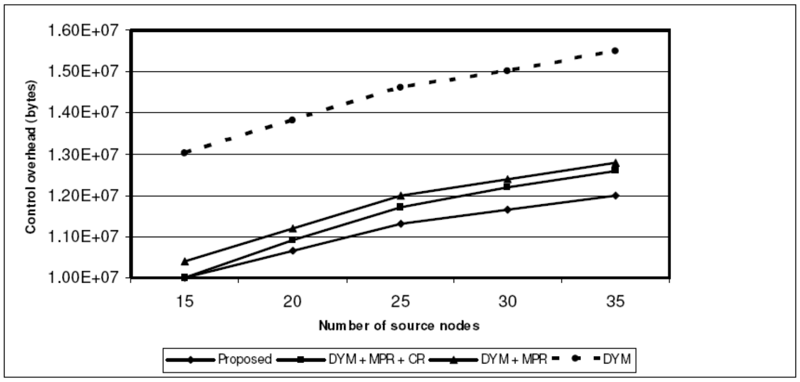

Fig. 5.3. *Control overhead (bytes) vs. number of data source nodes (75 nodes in the networks)*

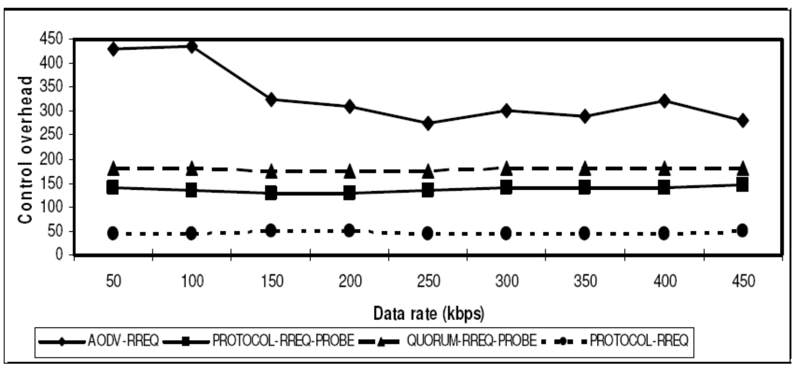

Fig. 5.4. *Control overhead (bytes) vs. data rate (kbps). Comparison of performance of the proposed protocol with the QUORUM protocol in [24]*

packets to its destination node. Each flow is alive for 10 minutes and each simulation run is executed for 15 minutes. The link robustness value is computed once per second and the value of α in EWMA is taken as 0.5. All these parameters are set as per simulation environment presented in [24]. For the purpose of comparison, only the RREQ messages and the probe packets in the protocols are considered since these broadcast messages largely contribute to the control overhead. Fig. 5.4 shows the overhead due to RREQ packets in AODV and the proposed protocol for different data rates. The control overhead of the proposed protocol is first evaluated only with the RREQ packets and then with RREQ packets and the probe packets together. This also gives an idea of the additional overhead introduced due to the probe packets. It can be easily observed that the proposed protocol has very low overhead even with the probe packets when compared with the naive AODV protocol. It is also worth observing that the proposed protocol has about 20% less control overhead that the protocol proposed in [24] due to its robust bandwidth estimation of the wireless links.

Fig. 5.5 shows that AODV has a very high overhead due to control packets for increasing number of flows in the system. AODV always tries to establish routing paths based on minimum hop-counts. It does not consider the aspect of link reliability. This leads to frequent selection of unreliable links and consequent link-breaks and consequent re-discovery of routes resulting in high overhead of control packets. In

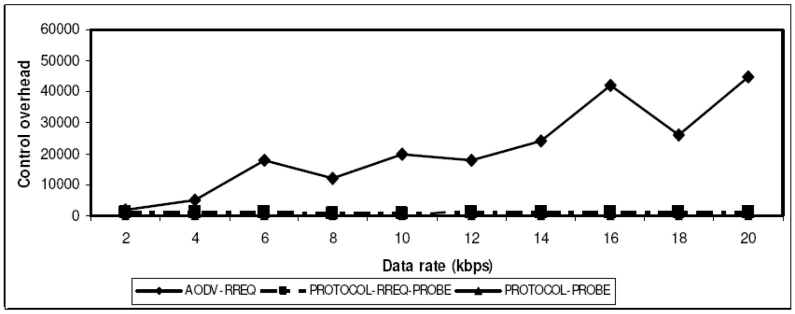

FIG. 5.5. *Control overhead vs. number flows in the network. Proposed protocol has much less control overhead than AODV protocol and has similar performance as that of QUORUM protocol in [24]*

contrast, the proposed protocol has a very limited control overhead since paths with higher link reliability only are selected for routing purpose. The algorithm proposed in [24] has similar performance as the proposed protocol in this case. The results clearly demonstrate while the proposed protocol has similar trends as the protocol in [24] as far as control overhead with number of flows in the network are concerned, it has almost 20% reduction in control overhead for a particular value of network flow when compared with the protocol in [24].

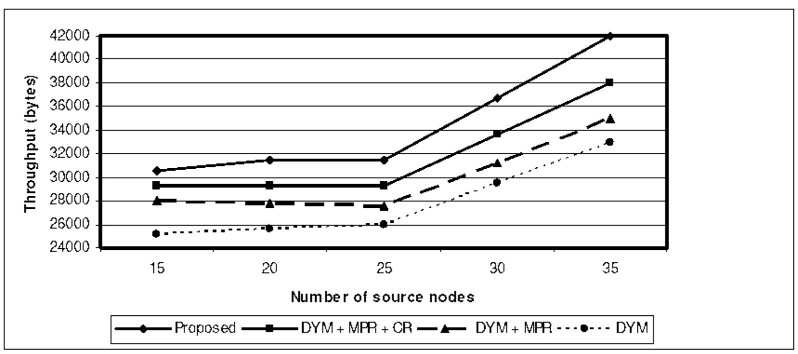

FIG. 5.6. *Network throughput in bits per second (BPS) vs. number of data source nodes (50 nodes in the network)*

5.2. Network Throughput. The performance of the protocol is also studied with respect to its ability to enhance network throughput. It may be intuitively clear that the reduction in control overhead should lead to a corresponding increase in the network throughput. Fig. 5.6 and Fig. 5.7 represent the data throughput in the network under varying number of source nodes with total number of nodes in the network being 50 and 75 respectively.

It may be observed that the proposed protocol produces maximum network throughput among all the four protocol studied. There are various factors that contribute to the enhanced throughput with the proposed protocol. First, the throughput significantly increases when MPRs are used due to reduced number of collision in the wireless medium and fewer retransmissions. Moreover, circular routing improves the performance further due to use of fixed network that has higher effective bandwidth.

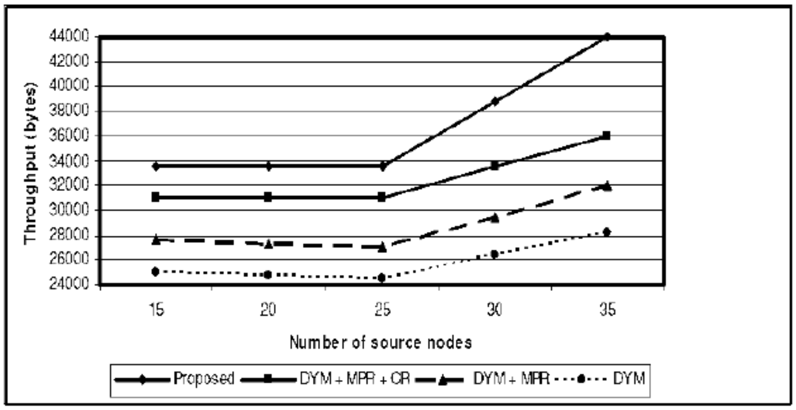

FIG. 5.7. *Network throughput in bits per second (BPS) vs. number of data source nodes (75 nodes in the network)*

Accurate estimate of link quality also contributes to higher throughput, since packets are always forwarded through the link that has the highest effective bandwidth. Finally, efficient bandwidth estimation ensures that there will be minimum packet retransmission.

5.3. End-to-End Delay Estimation. To demonstrate the effectiveness of the end-to-end delay estimation mechanism by probe packets mentioned in Section 4.3, delays estimated by nave RREP approach and the probe packet approach are compared with the actual end-to-end delay in the routing paths. The records are observed for different flow rates with each flow having a minimum bandwidth requirement of $B_{min} = 50$ Kbps.

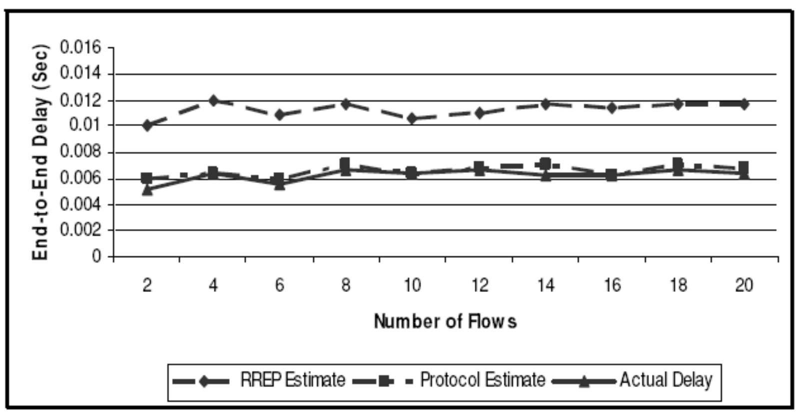

FIG. 5.8. *End-to-end delay estimation by different protocols for different number of nodes in the network*

Fig. 5.8 shows that the probe packet-based mechanism very accurately estimates the actual delay. The naive RREP approach is very poor in estimation of the delay as explained in Section 4.3.

5.4. Detection of Selfish Nodes. As mentioned in Section 4.7, the proposed protocol has the ability to detect selfish nodes which try to use network resources

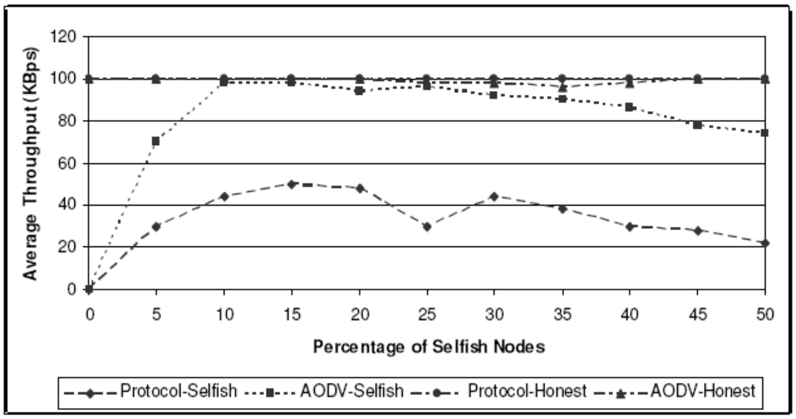

Fig. 5.9. *Average throughput for different protocols with varying number of selfish nodes*

without contributing to the cooperative framework of routing. To evaluate its detection capability of selfish nodes, two types of flows are distinguished: *selfish* and *honest*. A flow is considered selfish if either its source or destination is a selfish node, otherwise the flow is considered to be honest. Some mesh clients are selected randomly and configured as selfish nodes. In each of the 20 run of the simulation, 10 flows of 50 kbps data rate are generated randomly. The throughput in the network is measured under four different types of flows: (i) honest flows using proposed protocol, (ii) selfish flows (flows where selfish nodes are involved) using the proposed protocol, (iii) honest flows using simple AODV protocol [32], and (iv) selfish flows using AODV protocol.

It may be observed from Fig. 5.9 that AODV cannot restrict the traffic along the selfish flows. The selfish nodes can fully exploit the routing process to have their packets routed in the network. However, the proposed protocol reduces the flows along the selfish paths. In fact, the performance of AODV is not very much affected by presence of selfish nodes, since it never establishes routing path based on hello packets. Since the proposed protocol establishes route based on hello packets received form neighbors, its performance is affected by the presence of selfish nodes. However, its performance is not substantially affected, since most in most cases, these nodes are not allowed to participate in the routing, because of the low values of their link reliability. It may also be mentioned that the proposed protocol is able to maintain, on average, 35% more throughput in presence of selfish nodes when compared with the protocol proposed in [24]. The large difference is due to its ability to detect selfish nodes faster by its effective bandwidth estimation in the route where non-forwarding of packets is treated as packet drops due to congestion.

6. Conclusion and Future Work. WMNs have become an important focus area of research in recent years owing to their great promise in realizing numerous next-generation wireless services. Driven by the demand for rich and high-speed content access, recent research has focused on developing high performance communication protocols, while security and privacy issues have received relatively little attention. However, given the wireless and multi-hop nature of communication, WMNs are subject to a wide range of security and privacy threats. Accordingly, designing a high-performance, efficient, secure and user privacy-preserving routing protocol for

WMN is a very challenging task due to involvement of a number of complex factors. This paper has presented a routing protocol that has very low control overhead and high network throughput when the number of source nodes in a WMN is large. By robust estimation wireless link quality and the available bandwidth in the wireless route and exploiting the benefits of using MPRs and circular routing technique, the protocol is able to sustain a high level of throughput with a low control overhead. The user privacy is protected by using a novel anonymized authentication protocol. Simulation results have shown the protocol is more efficient than some of the existing routing protocols for WMNs. Future work includes developing a security module with the routing protocol that will be able to defend against tunnelling attack [33], in which two malicious nodes advertise in such a way as if they have a very reliable ink between them. This is achieved by tunnelling AODV messages between the nodes. No security scheme exists so far that can detect this attack promptly and efficiently.

REFERENCES

[1] F. J. Ross and P. M. Ruiz, A Low Overhead Architecture for Infrastructure-Based Wireless Mesh Networks, *Proceedings of the First International Workshop on Wireless Mesh: moving towards Applications (WiMeshNets'06*, Waterloo, Ontario, Canada, August, 2006.

[2] D. D. Couto, D. Aguqayo, J. Bricket, and R. Morris, A High - Throughput Path Metric for Multi-Hop Wireless Routing, *Proceedings of the 9th ACM Annual International Conference on Mobile Computing and Networking (MOBICOM'09)*, pp. 134 - 146, September, 2003.

[3] D. Aguqayo, J. Bricket, S. Biswas, G. Judd, and R. Morris, Link-Level Measurements from an 802.11b Mesh Network, *Proceedings of the ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'04)*, pp. 121 - 132, 2004.

[4] H. Badis, I. Gawedzki, and K. Al Agha, QoS Routing in Ad Hoc Networks Using QOLSR with No Need of Explicit Reservation, *Proceedings of the 60th IEEE Vehicular Technology Conference (VTC-Fall'04)*, Vol. 4, pp. 2654 - 2658, September, 2004.

[5] R. Draves, J. Padhye, and B. Zill, Comparison of Routing Metrics for Static Multi-Hop Wireless Networks, *Proceedings of ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'04*, pp. 133 - 144, 2004.

[6] R. Draves, J. Padhye, and B. Zill, Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks, *Proceedings of the 10th ACM Annual International Conference on Mobile Computing and Networking (MOBICOM'04)*, pp. 114- 122, 2004.

[7] Q. Xue and A. Ganz, QoS Routing for Mesh-Based Wireless LANs, *International Journal of Wireless Information Networks*, Vol. 9, No. 3, pp. 179 - 190, 2002.

[8] Q. Xue and A. Ganz, Ad Hoc QoS On-Demand Routing (AQOR) in Mobile Ad Hoc Networks, *Journal of Parallel and Distributed Computing*, Vol. 63, No. 2, pp. 154 - 165, February, 2003.

[9] Y. Yang, J. Wang, and R. Kravets, Interference-Aware Load Balancing for Multi-Hop Wireless Networks, *Technical Report, TR: UIUCDCS-R-2005*, University of Illinois, Arbana Champaign, 2005.

[10] K. Ramachandran, M. Buddhikot, G. Chandranmenon, S. Miller, E. Belding-Royer, and K. Almeroth, On the Design and Implementation of Infrastructure Mesh Networks, *Proceedings of IEEE Workshop on Wireless Mesh Networks (WiMesh'05)*, IEEE Press, 2005.

[11] J.-C. Chen, S. Li, S.- H. Chan, and J.- Y. He, WIANI: Wireless Infrastructure and Ad-Hoc Network Integration, *Proceedings of IEEE International Conference on Communications (ICC'05)*, Vol. 5, pp. 3623 - 3627, May, 2005.

[12] R.-H. Hwang, C.- Y. Wang, C.- Y. Li, Y.- S. Chen, Mobile IPv6-Based Ad Hoc Networks: Its Development and Applications, *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 11, pp. 2161 - 2171, November, 2005.

[13] C. Ahlund and A. Zaslavsky, Extending Global IP Connectivity for Ad Hoc Networks, *Kluwer Telecommunication Systems, Modeling, Analysis, Design and Management*, Vol. 24, No. 2, pp. 221 - 250, 2003.

[14] P. Ratnachandani and R. Kravets, A Hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks, *Proceedings of the IEEE Wireless Communications and Networking*

Conference (WCNC'03), Vol. 3, pp. 1522 - 1527, New orleans, Los Angeles, USA, March, 2003.

[15] Y. Sun, E. Belding-Royer, and C. Perkins, Internet Connectivity for Ad Hoc Mobile Networks, *International Journal of Wireless Information Networks*, Vol. 9, No. 2, pp. 75 - 88, 2002.

[16] M. Michalak and T. Braun, Common Gateway Architecture for Mobile Ad-Hoc Networks, *Proceedings of the 2nd Annual Conference on Wireless On-Demand Network Systems and Services (WONS'05)*, pp. 70 - 75, Washington DC, USA, January, 2005.

[17] R. Baumann, VANET: Vehicular Ad Hoc Networks, *Master's Thesis*, ETH, Zurich, 2004.

[18] B.- N. Cheng, M. Yuksel, and S. Kalyanaraman, Orthogonal Rendezvous Routing Protocol for Wireless Mesh Networks, *IEEE / ACM Transactions on Networking*, Vol. 17, No. 2, pp. 542 - 555, April, 2009.

[19] M. Mosko and J. J. Garcia-Luna-Aceves, Ad Hoc Routing with Distributed Ordered Sequences, *Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM'06)*, pp. 1 -12, Barcelona, Spain, April, 2006.

[20] M. Mosko and J. J. Garcia-Luna-Aceves, Multipath Routing in Wireless Mesh Networks, *Proceedings of the First IEEE Workshop on Wireless Mesh Networks (WiMesh)*, Santa Clara, California, USA, September, 2005.

[21] H. Ju and I. Rubin, Backbone Topology Synthesis for Meshed Wireless LANs, *Proceedings of IEEE International Conference on Computer Communications (INFOCOM'06)*, Barcelona, Spain, April, 2006.

[22] R. Baumann, S. Heimlicher, V. Lenders, and M. May, HEAT: Scalable Routing in Wireless Mesh Networks Using Temperature Field, *Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'07)*, pp. 1 - 9, Espoo, Finland, June, 2007.

[23] H. Lundgren, E. Nordstrom, and C. Tschudin, The Gray Zone Problem in IEEE 802.11b Based Ad Hoc Networks, *ACM SIGMOBILE Mobile Computing and Communications Review, (MC2R)*, Vol. 6, No. 3, pp. 104 - 105, July, 2002.

[24] V. Kone, S. Das, B. Y. Zhao, and H. Zhang, QUORUM: Quality of Service in Wireless Mesh Networks, *Journal of Mobile Networks and Applications*, Vol. 12, No. 5 - 6, pp. 358 - 369, 2007.

[25] T. Clausen and P. Jacquet, Optimized Link State Routing Protocol, *IETF RFC 3626*, 2003.

[26] F. Yang, Q. Zhang, W. Zhu, and Y.- Q. Zhang, End-to-End TCP-Friendly Streaming Protocol and Bit Allocation for Scalable Video over Wireless Internet, *IEEE Journal of Selected Areas in Communications*, Vol. 22, No. 4, pp. 777 - 790, May, 2004.

[27] L. Santhanam, B. Xie, and D. Agrawal, Selfishness in Mesh Networks: Wired Multi-Hop MANETS, *IEEE Journal of Wireless Communications*, Vol. 15, No. 4, pp. 16 - 23, August, 2008.

[28] T. Cao, D. Lin, and R. Xue, Improved Ring Authenticated Encryption Scheme, *Proceedings of the 10th Joint International Computer Conference*, pp. 341 - 346, Kunming, China, 2004.

[29] R. Rivest, A. Shamir, and Y. Tauman, How to Leak a Secret, *Advances in Cryptology, ASIACRYPT, LNCS*, Vol. 2248, pp. 552 - 565, Springer, Heidelberg, 2001.

[30] Network Simulator Qualnet, URL: http://www.scalable-networks.com.

[31] F. Ross, Dymoum Implementation, URL: http://masimum.dif.um.es/?Software:DYMOUM.

[32] C. E. Perkins and E. M. Royer, Ad-Hoc On-Demand Distance Vector Routing, *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systes and Applications (WMCSA'99)*, pp. 90 - 100, New Orleans, Los Angeles, USA, February, 1999.

[33] C. Li, Z. Wang, and C. Yang, Secure Routing for Wireless Mesh Networks, *International Journal of Network Security*, Vol. 13, No. 2, pp. 1 - 12, September, 2011.